CLAIMS

1. Method for device-type authentication in a communication system, comprising the steps of:

providing, in a first device connected to said communication system, first header information of a communication message;

5

10

15

20

25

said first header information being related with a device-type associated commitment;

tamper-resistantly creating a first signature in said first device based on at least tamper-resistant device-type specific information of said first device;

providing, in said first device, second header information of said communication message comprising said signature;

communicating said communication message to a second device connected to said communication system; and

authenticating said first header information by verifying said first signature after said communicating step.

- 2. Method according to claim 1, wherein said communication system is based on a transfer protocol selected from the group: of HyperText Transfer Protocol and Simple Mail Transfer Protocol.
- 3. Method according to claim 2, wherein said device-type associated commitment is a commitment to follow Digital Rights Management compliance.
- 4. Method according to claim 1, wherein said first device is a user terminal.
- 5. Method according to claim 1, wherein said second device is a server.

- 6. Method according to claim 1, wherein said device-type specific information comprises a definition of an algorithm according to which said signature is to be created.
- 7. Method according to claim 1, wherein said device-type specific information comprises a data string being unique for each particular device type.

5

10

15

20

25

30

- 8. Method according to claim 1, wherein said step of creating a signature is additionally based on at least one item in the group of: time, date and header information.
- 9. Method according to claim 1, wherein said step of authenticating in turn comprises the steps of:

determining, in said second device, a device-type of said first device based on said first header information;

creating a second signature in said second device based on at least tamper-resistant information associated with said determined device-type; and accepting said determined device-type as authentic if said first and second signatures agree.

10. Method according to claim 1, wherein said step of authenticating in turn comprises the steps of:

forwarding information about said first header information and said first signature from said second device to a third device connected to said communication system;

requesting a verification of the authenticity of said first header information by said third device; and

accepting said first header information as authentic if said third device provides a positive verification.

11. Method according to claim 10, wherein said third device is associated with a manufacturer of said first device.

12. Communication device connectable to a communication system, comprising:

means for providing first header information of a communication message;

said first header information being related with a device-type associated commitment;

tamper-resistant storage of device-type specific information of said communication device;

tamper-resistant signature generator, arranged to create a first signature based on at least said device-type specific information;

means for providing second header information of said communication message comprising said signature; and

communication means for communicating said communication message to another device connected to said communication system.

- 13. Communication device according to claim 12, wherein said communication means is arranged to support a transfer protocol selected from the group: of HyperText Transfer Protocol and Simple Mail Transfer Protocol.
- 14. Communication device according to claim 13, further comprising Digital Rights Management means, whereby said device-type associated commitment is a commitment to follow Digital Rights Management compliance.
- 15. Communication device according to any of the claims 12 to 14, wherein said communication device is a user terminal.
- 16. Communication device connectable to a communication system, comprising:

communication means for receiving a communication message from a sending device connected to said communication system;

20

5

10

15

25

30

said communication message comprising first header information being related with a device-type associated commitment;

said communication message further comprising second header information in turn comprising a first signature; and

authenticating means arranged to verify said first signature.

5

10

15

20

25

30

17. Communication device according to claim 16, wherein said authenticating means in turn comprises:

means for determining a device-type of said sending device based on said first header information;

storage of device-type specific information of communication devices;

signature generator, arranged to retrieve device-type specific information corresponding to said determined device-type;

said signature generator being further arranged to create a second signature based on said retrieved device-type specific information; and

means for accepting said determined device-type as authentic if said first and second signatures agree.

18. Communication device according to claim 16, wherein said authenticating means in turn comprises:

means for forwarding information about said first header information and said first signature to a further device connected to said communication system;

means for requesting a verification of the authenticity of said first header information by said further device; and

means for accepting said first header information as authentic if said further device provides a positive verification.

19. Communication device according to claim 16, wherein said communication means is arranged to support a transfer protocol selected from the group: of HyperText Transfer Protocol and Simple Mail Transfer Protocol.

- 20. Communication device according to claim 19, further comprising Digital Rights Management means, whereby said device-type associated commitment is a commitment to follow Digital Rights Management compliance.
- 21. Communication device according to any of the claims 16 to 20, wherein said communication device is a server.

5